IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A wireless communication system including a plurality of terminals, comprising:

an ad-hoc network;

a first terminal configured to send, using the ad-hoc network, a signal that includes beacon information having a first identifier that identifies the origin of the sent beacon and a second identifier that identifies an issuing terminal of a certificate of privilege; and

a second terminal configured to send, using the ad-hoc network, an authentication request to the first terminal in response to the signal sent from the first terminal by providing the certificate of privilege which matches the second identifier,

wherein the certificate of privilege includes encrypted data for certifying the second terminal, ~~and~~ the second terminal comprising:

a certificate-of-privilege issuing terminal list table for storing a public key certificate of a terminal that has issued the certificate of privilege;

authentication-request receiving means for receiving a second authentication request from the first different terminal in response to the authentication request sent from the authentication request means;

verification means for verifying a second certificate of privilege contained in the second authentication request received by the authentication-request receiving means by using a public key contained in the public key certificate stored in the certificate-of-privilege issuing terminal list table; and

operation-mode checking means for determining, after the second certificate of privilege is successfully verified by the verification means, that the second authentication

request is rejected when the operation mode of the different terminal is not permitted by an operable mode contained in the second certificate of privilege~~—, thereto~~.

Claims 2-12 (Cancelled).

Claim 13 (Previously Presented): A terminal according to claim 1, wherein:

the identifier is a terminal identifier of the terminal that has issued the certificate of privilege; and

the certificate-of-privilege issuing terminal list table stores the terminal identifier of the terminal that has issued the certificate of privilege, the public key certificate of the terminal that has issued the certificate of privilege, and a storage location of the certificate of privilege in the certificate of privilege table in association with each other.

Claim 14 (Previously Presented): A terminal according to claim 1, further comprising:

a policy table for storing a management policy to be used with the different terminal; and

management-policy setting means for setting a management policy contained in the second certificate of privilege in the policy table when the operation-mode checking means determines that the second authentication request is not rejected.

Claims 15-22 (Cancelled).

Claim 23 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a plurality of certificates of privilege indicating an access right of the terminal;

a status table for storing an operation mode of the terminal;

selection means for providing an instruction to select one of the plurality of certificates of privilege stored in the certificate of privilege table; and

sending means for sending a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second identifier that identifies an issuing terminal of a the certificate of privilege selected by the selection means and the operation mode of the terminal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal, ~~and~~ the second terminal comprising:

a certificate-of-privilege issuing terminal list table for storing a public key certificate of a terminal that has issued the certificate-of-privilege;

authentication-request receiving means for receiving a second authentication request from the first different terminal in response to the authentication request sent from the authentication request means;

verification means for verifying a second certificate of privilege contained in the second authentication request received by the authentication-request receiving means by using a public key contained in the public key certificate stored in the certificate-of-privilege issue terminal list table; and

operation-mode checking means for determining, after the second certificate of privilege is successfully verified by the verification means, that the second authentication request is rejected when the operation mode of the different terminal is not permitted by an operable mode contained in the second certificate of privilege~~—, thereto~~.

Claim 24 (Original): A terminal according to claim 23, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claims 25-26 (Cancelled).